DASTRA

Les cinq documents indispensables en cas de contrôle de la CNIL

5 Avril 2022

DPO FORUM

Présentation

Jérôme DE MERCEY
Co-fondateur de Dastra

Droit

DPO

Service des contrôles

Droit du Numérique

Protection des données

CNIL

DASTRA

Table des matières

L'implication des opérationnels dans la préparation aux contrôles de la CNIL : une étape cruciale vers l'accountability

Les **principaux facteurs** ralentissant la mise en conformité sont :

- La **charge de travail** pour les DPOs (66%)
- La **complexité** du Règlement (39%)

Parmi les étapes les **moins avancées** figurent :

- les **analyses d'impact** relatives à la protection des données (42%)
- la mise en place des **durées de conservation** (30%)
- le **privacy by design** (21%).

Mettre en place et maintenir la conformité RGPD impose **de mettre en place des processus outillés** permettant à **toutes les personnes impliquées** dans la protection des données **d'agir** de concert, sous l'orchestration du DPO

Source: KPMG – Baromètre RGPD : 3 ans après où en êtes-vous ?

Table des matières

Les contrôles de la CNIL

- La **CNIL** : autorité administrative indépendante créée en 1978.
- Dispose du pouvoir de contrôle des organismes privés depuis 2004.
- Pouvoirs de contrôle inscrits dans le RGPD (article 58-1), la loi du 6 janvier 1978 modifiée (article 19) et le décret du 29 mai 2019 (articles 16 et suivants).
- Réalise environ 300 contrôles par an.
- Les entités contrôlées sont rendues publiques en open data.

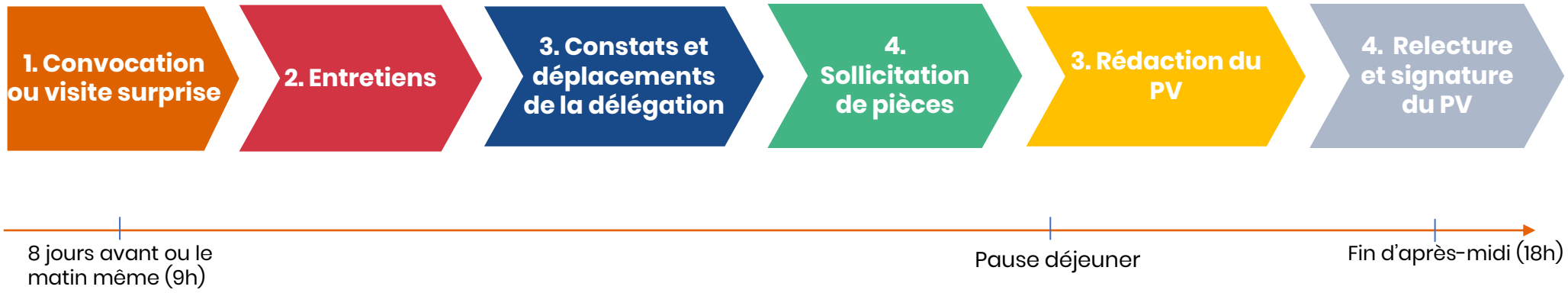
CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

4 formes de contrôle :

- Contrôle sur place
- Contrôle en ligne
- Contrôle sur audition
- Contrôle sur pièces

Le déroulé d'un contrôle (1/2)

Contrôle sur place ou sur audition



Pièces indispensables :

1. Le registre des activités de traitement
2. Le registre des violations de données
3. Les analyses d'impact sur la protection des données (PIA)
4. Les contrats avec les sous-traitants
5. Les procédures et politiques internes

Le déroulé d'un contrôle (2/2)

Contrôle en ligne

1. Visite du site internet ou de l'application
2. Réception du PV de constats et des pièces
3. Demandes complémentaires

Contrôle sur pièce

1. Courrier de la CNIL
2. Questions
3. Réponses aux questions

Comment arrive-t-on à être contrôlé ?

Plusieurs sources de contrôle :

- **Le programme annuel des contrôles**
- **Les réclamations et les signalements**
- **Les initiatives**
- **Les dispositifs de vidéoprotection**
- **Les procédures de contrôle clôturées, les mises en demeure et les sanctions**

Table des matières

1

Le registre des activités de traitement

En pratique, il y a deux registres

RT

Le « fichier des fichiers » est une obligation du RGPD. L'article 30.1 prévoit un socle minimum d'informations à apporter pour chaque traitement :

- Le nom et les coordonnées du responsable du traitement
- Le nom et les coordonnées du DPO le cas échéant
- Le nom et les coordonnées du représentant au sein de l'UE le cas échéant
- Les finalités du traitement
- Les catégories de personnes concernées
- Les catégories de données personnelles
- Les catégories de destinataires et les transferts hors UE/EEE
- Les durées de conservation des données
- Les mesures de sécurité mises en œuvre

ST

Le registre en tant que sous-traitant. L'article 30.2 prévoit un socle minimum d'informations à apporter pour chaque traitement :

- Le nom et les coordonnées de chaque responsable du traitement ou sous-traitant pour le compte duquel il agit
- Le nom et les coordonnées du DPO le cas échéant
- Le nom et les coordonnées du représentant au sein de l'UE le cas échéant
- Les catégories de traitements effectués
- Les transferts hors UE/EEE
- Les mesures de sécurité mises en œuvre

2

Le registre des violations de données

Le registre des violations est prévu par l'article 33 du RGPD et doit notamment contenir les éléments suivants :

- la nature de la violation ;
- les catégories et le nombre approximatif des personnes concernées ;
- les catégories et le nombre approximatif de fichiers concernés ;
- les conséquences probables de la violation ;
- les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation ;
- le cas échéant, la justification de l'absence de notification auprès de la CNIL ou d'information aux personnes concernées.

3

Les analyses d'impact sur la protection des données (PIA)

3 grandes étapes :

1. Description systématique du traitement
2. Evaluation de la nécessité et de la proportionnalité
3. Les risques pour les droits et libertés des personnes concernées sont gérés (accès illégitime aux données, modification non désirée des données, disparition des données)

Notre guide pratique sur : https://www.dastra.eu/fr/guide/guide-pratique-analyse-impact-protection-des-donnees/499

4

Les contrats avec les sous-traitants

et les responsables conjoints

Tous les contrats avec les sous-traitants doivent inclure des clauses obligatoires prévues à l'article 28 du RGPD.

Le contrat doit définir :

- l'objet et la durée de la prestation
- la nature et la finalité du traitement
- le type de données à caractère personnel traitées
- les catégories de personnes concernées
- les obligations et les droits du responsable de traitement
- les obligations et les droits du sous-traitant tels que prévus à l'article 28 du règlement

5

Les procédures et politiques internes

Des preuves de la mise en œuvre du principe de responsabilité (accountability)

- Procédure de gestion de l'exercice des droits des personnes
- Procédure de gestion des violations de données
- Politique de protection des données personnelles
- Audit de conformité
- Politique de sécurité
- etc.

Table des matières

« Lessons learned »

1

Obligation « ex ante »

Le RGPD est une obligation de conformité qui nécessite d'être « accountable » à tous les niveaux de l'organisation, depuis les opérationnels jusqu'aux décisionnaires

2

Des écarts de conformité systématiques

Manque de connaissance, pilotage et de mise en œuvre notamment sur les durées de conservation des données, la transparence et la sécurité des données

3

Une nécessité d'anticiper sur le long-terme

Malgré des ressources motivées et performantes, plusieurs années sont nécessaires pour se mettre en conformité, sans compter le maintien à jour de la documentation au fur et à mesure de l'évolution des projets informatiques

4

L' apport indispensable des outils technologiques

L'implication des opérationnels dans les processus RGPD et la mise en place et le maintien de la conformité RGPD impose de mettre en place des processus outillés permettant à toutes les personnes impliquées dans la protection des données d'agir de concert, sous l'orchestration du DPO

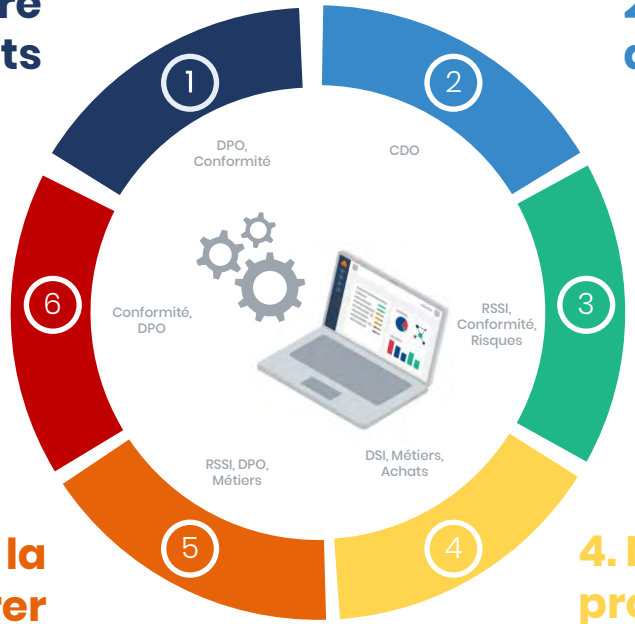
La gestion du RGPD : plus qu'un projet, un processus continu nécessitant l'implication de toute l'entreprise

Le **Data Protection Officer (DPO)** est le référent responsable au sein des organismes de la bonne mise en œuvre du RGPD. Qu'il soit nommé ou non, les organisations doivent :

1. Documenter le registre des traitements

2. Cartographier les données personnelles

6. Piloter la conformité, suivre la progression & contrôler



3. Auditer, analyser les risques & réaliser les PIA

5. Planifier la remédiation & orchestrer la conformité

4. Mettre en œuvre les processus obligatoire
(exercices de droit, violation de données, privacy by design...)

Dastra est une plateforme RGPD complète, collaborative et flexible

Dastra permet à votre organisation de répondre à **toutes les obligations du RGPD**, d'améliorer la **productivité** et de **valoriser** la **protection des données** de votre organisation.

- REGISTRE DES TRAITEMENTS
- ANALYSES D'IMPACT & AUDITS
- DEMANDES D'EXERCICES DE DROIT
- VIOLATIONS DE DONNÉES
- TABLEAU DE BORD
- CARTOGRAPHIE DES DONNÉES
- GESTION DES RISQUES
- CONSENTEMENT COOKIES

En savoir plus

Tout est accessible sur :

- ✓ https://www.dastra.eu/fr

- ✓ Création d'un compte gratuit sur dastra.eu/signup

Le programme annuel des contrôles de la CNIL

- ✓ https://www.cnil.fr/fr/cybersecurite-donnees-de-sante-cookies-les-thematiques-prioritaires-de-controle-en-2021

La liste des organismes contrôlés

- ✓ https://www.data.gouv.fr/fr/datasets/controles-realises-par-la-cnil/

La charte des contrôles de la CNIL

- ✓ https://www.cnil.fr/fr/autres-referentiels

Des questions ?

DASTRA

Transformez vos contraintes RGPD en accélérateur avec la solution Dastra

Contactez nous

Essayez gratuitement